FILED
FEB 21 2007
OFFICE OF THE CLERK
SUPREME COURT, U.S.

(2)

No. 06-867

In the Supreme Court of the United States

ELOUISE PEPION COBELL, ET AL., PETITIONERS

v.

DIRK KEMPTHORNE, SECRETARY OF THE INTERIOR, ET AL.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

BRIEF FOR THE RESPONDENTS IN OPPOSITION

PAUL D. CLEMENT
Solicitor General
Counsel of Record
PETER D. KEISLER
Assistant Attorney General
ROBERT E. KOPP
MARK B. STERN
THOMAS M. BONDY
ALISA B. KLEIN
MARK R. FREEMAN
ISAAC J. LIDSKY
Attorneys
Department of Justice
Washington, D.C. 20530-0001
(202) 514-2217

QUESTION PRESENTED

Whether the court of appeals erred in vacating an injunction that required the Department of the Interior to disconnect nearly all of its major computer systems from the internet, from other federal agencies, and from internal Department connections.

TABLE OF CONTENTS

Page

Opinions below 1
Jurisdiction 1
Statement 2
Argument 9
Conclusion 18

TABLE OF AUTHORITIES

Cases:

Brooks, In re, 383 F.3d 1036 (D.C. Cir. 2004), cert. denied, 543 U.S. 1150 (2005) 3

Cobell v. *Kempthorne*, 455 F.3d 317 (D. C. Cir. 2006), petition for cert. pending, No. 06-868 (filed Dec. 19, 2006) 3, 4, 15

Cobell v. *Norton*:

240 F.3d 1081 (D.C. Cir. 2001) 2

274 F. Supp. 2d 111 (D.D.C. 2003), superseded, 310 F. Supp. 2d 98 (D.D.C.), vacated and remanded, 391 F.3d 251 (D.C. Cir. 2004) 4, 5

310 F. Supp. 2d 98 (D.D.C.) vacated and remanded, 391 F.3d 251 (D.C. Cir. 2004) 5

334 F.3d 1128 (D.C. Cir. 2003) 3

391 F.3d 251 (D. C. Cir. 2004) 3, 5, 13

392 F.3d 461 (D.C. Cir. 2004) 17

428 F.3d 1070 (D.C. Cir. 2005) 2, 3

Firestone Tire & Rubber Co. v. *Bruch*, 489 U.S. 101 (1989) 16

Kempthorne, In re, 449 F.3d 1265 (D.C. Cir. 2006) 3

Cases—Continued: Page

Nevada v. *United States*, 463 U.S. 110 (1983) 16
Norton v. *Southern Utah Wilderness Alliance*, 542 U.S. 55 (2004) 17
United States v. *Mason*, 412 U.S. 391 (1973) 16, 17
Weinberger v. *Romero-Barcelo*, 456 U.S. 305 (1982) . 12, 13

Statutes and regulations:

Administrative Procedure Act, 5 U.S.C. 701 *et seq.* 16
5 U.S.C. 706(1) 2
American Indian Trust Fund Management Reform Act of 1994, Pub. L. No. 103-412, 108 Stat. 4239 (25 U.S.C. 4001 *et seq.*) 2
§ 102(a), 108 Stat. 4240 2
Federal Information Security Management Act of 2002, 44 U.S.C. 3541 *et seq.* (Supp. III 2003) 10
44 U.S.C. 3541(1) (Supp. III 2003) 11
44 U.S.C. 3542(a) (Supp. III 2003) 11
44 U.S.C. 3543(a)(5) (Supp. III 2003) 11
44 U.S.C. 3544(a)(1)(A) (Supp. III 2003) 11
44 U.S.C. 3544(a)(2)(A) (Supp. III 2003) 11
44 U.S.C. 3544(a)(2)(B) (Supp. III 2003) 11
44 U.S.C. 3544(b)(8) (Supp. III 2003) 12
44 U.S.C. 3545 (Supp. III 2003) 11
18 U.S.C. 1030 (2000 & Supp. IV 2004) 12
44 U.S.C. 3502(4) 11

Miscellaneous: Page

H.R. Rep. No. 499, 102d Cong., 2d Sess. (1992) 2
Restatement (Second) of Trusts (1959) 17

In the Supreme Court of the United States

No. 06-867

ELOUISE PEPION COBELL, ET AL., PETITIONERS

v.

DIRK KEMPTHORNE, SECRETARY OF THE INTERIOR, ET AL.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

BRIEF FOR THE RESPONDENTS IN OPPOSITION

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. 1a-35a) is reported at 455 F.3d 301. The opinion of the district court (Pet. App. 36a-280a) is reported at 394 F. Supp. 2d 164.

JURISDICTION

The judgment of the court of appeals was entered on July 11, 2006. A petition for rehearing was denied on September 26, 2006 (Pet. App. 281a-282a). The petition for a writ of certiorari was filed on December 19, 2006. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

STATEMENT

In October 2005, as part of an ongoing class action seeking an accounting of funds held in trust for individual Indians by the government, the district court issued an injunction requiring the Department of the Interior (DOI) to disconnect most of its major computer systems from each other, from the internet, and from other federal agencies. Pet. App. 36a-280a. The court of appeals vacated the injunction, *id.* at 1a-35a, holding that "the equities and harms involved in this case do not, on balance, justify requiring [DOI] to take such a drastic step," *id.* at 34a.

1. DOI administers approximately 260,000 Individual Indian Money (IIM) trust accounts with balances totaling approximately $400 million. See 05-5269 C.A. App. 52 (455 F.3d 317 (D.C. Cir. 2006)); H.R. Rep. No. 499, 102d Cong., 2d Sess. 2 (1992); 428 F.3d 1070, 1072 (D.C. Cir. 2005). In 1994, Congress enacted the American Indian Trust Fund Management Reform Act of 1994, Pub. L. No. 103-412, 108 Stat. 4239 (25 U.S.C. 4001 *et seq.*), which requires the Secretary of the Interior to "account for the daily and annual balance of all funds held in trust by the United States for the benefit of an Indian tribe or an individual Indian which are deposited or invested pursuant to" a 1938 statute addressing investment of trust monies. § 102(a), 108 Stat. 4240 (25 U.S.C. 4011(a)). In 1996, a class of present and former IIM accountholders filed this lawsuit, asserting that the government had failed to provide a timely, adequate accounting. In 2001, the court of appeals held that the agency's performance of required accounting activities had been "unreasonably delayed" within the meaning of 5 U.S.C. 706(1). 240 F.3d 1081, 1108 (D.C. Cir. 2001).

On eight subsequent occasions, including in the decision below, the court of appeals vacated or set aside district court orders directed against DOI and senior government officials. See 334 F.3d 1128, 1137-1150 (D.C. Cir. 2003) (reversing an order of contempt against the Secretary and Assistant Secretary, and issuing a writ of mandamus to direct the removal of a "Special Master-Monitor" appointed by the district court); *In re Brooks*, 383 F.3d 1036, 1044-1046 (D.C. Cir. 2004) (granting a writ of mandamus to recuse another court-appointed special master from contempt proceedings), cert. denied, 543 U.S. 1150 (2005); 391 F.3d 251, 258-262 (D.C. Cir. 2004) (vacating an injunction requiring DOI to disconnect its computers from the internet); 392 F.3d 461, 465-478 (D.C. Cir. 2004) (vacating a structural injunction purporting to dictate the scope and methods of DOI's accounting activities and to enforce compliance with DOI's fiduciary responsibilities); 428 F.3d at 1074-1079 (vacating the accounting portion of the same structural injunction after the district court reissued it verbatim); *In re Kempthorne*, 449 F.3d 1265, 1268-1272 (D.C. Cir. 2006) (granting a writ of mandamus to recuse a special master and to suppress tainted reports); Pet. App. 1a-35a (vacating an injunction requiring DOI to disconnect its computers from the internet, as well as from all internal networks); 455 F.3d 317, 319, 323-325 (D.C. Cir. 2006) (vacating an injunction requiring DOI to include, in all communications with class members, a notice declaring that all trust-related information from DOI "may be unreliable"), petition for cert. pending, No. 06-868 (filed Dec. 19, 2006). In July 2006, the court of appeals

directed that the case be reassigned to a different district court judge. See *id.* at 325-336.[1]

2. The instant petition arises from petitioners' contention that DOI's computer systems for storing and processing individual Indian trust data (IITD) lack adequate security, thereby potentially undermining petitioners' right to an accounting.

a. In November 2001, a special master appointed by the district court issued a report identifying weaknesses in DOI's computer security that the special master believed could detrimentally affect the integrity of IITD. See Pet. App. 37a-39a. Although no evidence indicated that any person other than the special master had ever hacked into DOI's systems, the district court entered a temporary restraining order requiring DOI immediately to disconnect from the internet all information systems housing or providing access to IITD. *Id.* at 39a. To regain internet access, DOI agreed to a consent order by which it assented to a procedure for restoring internet connections with the approval of the special master. *Id.* at 39a-42a. Ultimately, most systems taken off-line were restored. *Id.* at 42a.

In July 2003, however, the district court entered a preliminary injunction under which the court, rather than the special master, assumed full authority over internet access. 274 F. Supp. 2d 111 (D.D.C.). The order made no provision for further reconnections as contemplated by the earlier consent agreement, but instead required immediate disconnection from the internet of the systems already approved by the special master. See *id.* at 135. The district court initially stayed aspects

[1] That reassignment order is the subject of a separate petition for a writ of certiorari, which is currently pending before this Court. See No. 06-868 (filed Dec. 19, 2006).

of its order to allow DOI to submit evidence showing that the systems still connected to the internet were secure from access by unauthorized users. *Id.* at 135-136. In March 2004, the district court issued a superseding preliminary injunction that required DOI immediately to disconnect all of its information systems from the internet, with limited exceptions. 310 F. Supp. 2d 98, 100-102 (D.D.C.).

b. In December 2004, the court of appeals vacated that injunction. 391 F.3d 251 (D.C. Cir.). Noting that "there was no evidence that anyone other than the Special Master's contractor had 'hacked' into any [DOI] computer system housing or accessing IITD," *id.* at 259, the court remanded for further proceedings, *id.* at 262.

On remand, the district court held a 59-day evidentiary hearing on DOI's information security. Pet. App. 14a. At the hearing, petitioners relied principally on the results of independent "penetration tests" performed by DOI's Inspector General (IG) at the request of the Assistant Secretary. *Id.* at 117a & n.17. To conduct the penetration tests, the IG had retained expert security consultants to conduct a variety of attacks simulated by "hackers." *Id.* at 117a. At the hearing, personnel from the IG's office and its contractors testified concerning the results of the penetration tests, their concerns about DOI's computer security, as well as the progress that the agency had made. See *id.* at 117a-163a; see also, *e.g.*, 05-5388 C.A. App. 1175-1176, 1385-1396.

3. In October 2005, the district court issued a new injunction requiring disconnection from the internet of nearly all of DOI's computers and computer systems.

See 394 F. Supp. 2d 164, 276-280 (D.D.C.).[2] Unlike the court's previous injunctive orders, that injunction required DOI to sever *internal* connections with other DOI computers, networks, and electronic devices. See *id.* at 277-278. The district court did not find that anyone other than the IG (and earlier the special master) had hacked into any relevant computer system, or that any IIM accountholder had been injured because of a problem with DOI's computer security. The court acknowledged that DOI "has made substantial progress in implementing a comprehensive departmental IT security program in a very short time," Pet. App. 221a, and it recognized that the agency's "progress in a period of five years is laudable," *id.* at 271a. The court also noted that DOI had invested more than $100 million in computer security during a three-year period. *Id.* at 262a. Despite the "substantial progress that has been made," however, the court concluded that a disconnection order was warranted because "the evidence indicates that [DOI] has not properly emphasized IITD in its IT security efforts." *Id.* at 271a-272a.

The district court ordered that DOI "forthwith" disconnect any computer that housed or provided access to IITD from the internet, from all internal networks, from all other information technology systems, and from any contractors, Tribes, or other third parties. 394 F. Supp. 2d at 277-278. The injunction exempted from its scope only those systems "necessary for protection against fires or other such threats to life, property, or national security," *id.* at 278, and it extended by its terms until

---

[2] Although the text of the district court's actual injunction is not reproduced in the appendix to the petition for a writ of certiorari, it appears as an addendum to the published version of the court's opinion.

such time as DOI could persuade the court, after further discovery and hearings, to authorize reconnection on a system-by-system basis, *id.* at 279. The injunction allowed DOI to reconnect computer systems for up to five business days per month "for the purpose of receiving and distributing trust funds, or for the purpose of conducting other necessary financial transactions." *Id.* at 278. Before reconnecting those systems, however, DOI was required to provide five days' advance notice to the court and to petitioners, together with a plan for interim "security controls and measures to cover such reconnection." *Id.* at 279.

4. The court of appeals stayed the district court's injunction pending appeal, see Orders of Oct. 21, 2005, and Dec. 9, 2005, and it ultimately vacated the injunction. Pet. App. 1a-35a. The court acknowledged "the possibility that [an intruder] may indeed hack into [DOI's] systems and even alter IITD, especially given that the spotlight of this litigation may make [DOI's] systems an inviting target." *Id.* at 30a. The court held, however, that the concerns identified in the district court's opinion "lack the specificity needed to justify injunctive relief, especially given the magnitude of the harm that this injunction would cause [DOI]." *Ibid.* The court emphasized that petitioners had "pointed to no evidence showing that anyone has already altered IITD by taking advantage of [DOI's] security flaws, nor that such actions are imminent." *Ibid.* The court also observed that it had "been shown no reason to believe that the effects" of any security breach that might occur "would likely be so extensive as to prevent the class members from receiving the accounting to which they are entitled." *Ibid.* Under those circumstances, the court explained,

> [t]he inherently imperfect nature of IT security means that if we granted injunctive relief here, based only on [DOI's] security vulnerabilities and not on a showing of some imminent threat or specific reason to be concerned that IITD is a target, we would essentially be justifying perpetual judicial oversight of [DOI's] computer systems.

Id. at 31a.

The court of appeals also held that the district court had failed adequately to consider "the immensity of the disruption" that the injunction would cause to DOI's operations. Pet. App. 31a-32a. The court of appeals found it likely "that a very high percentage of [DOI's] IT systems would be subject to disconnection, with serious consequences." *Id.* at 32a. The court noted in that regard that the injunction would require DOI to disconnect the computer systems that disburse more than $500 million each month in mineral revenues to States, Indians, and Treasury accounts. *Id.* at 32a-33a. The court concluded "that the harm [DOI] would immediately face upon complying with the disconnection order outweighs the class members' need for an injunction." *Id.* at 34a. The court of appeals also stated that, "in light of the far-reaching effects [the injunctive] order would have on [DOI's] operations," the court was "skeptical" of the district court's determination that the injunction would serve the public interest. *Ibid.* Accordingly, "[d]ue to the significant harm that this injunction would cause to [DOI] and the paucity of evidence that the class members' right to an accounting would be harmed without injunctive relief," the court of appeals vacated the injunction and remanded the case to the district court. *Id.* at 35a.

ARGUMENT

The decision of the court of appeals is correct and does not conflict with any decision of this Court or any other court of appeals. Further review is not warranted.

1. Petitioners' attacks on the decision below should not obscure the extraordinary nature of the injunction entered by the district court. Concerned that a "hacker" or disgruntled employee might access and manipulate trust-related data, the district court ordered an entire Cabinet agency to disconnect nearly all of its computer systems from the internet; to cut off electronic connections with other federal agencies, essential contractors, and the public that it serves; and to disassemble much of its internal electronic communications network. See 394 F. Supp. 2d 164, 276-280 (D.D.C. 2005). The court of appeals correctly held that any benefit to petitioners that the injunction might provide was too slight and too speculative to justify the disruption of DOI's functions that the order would entail.

a. As the court of appeals explained, the district court "disregarded the harm [the] injunction would cause to [DOI] and those depending on [DOI's] services" and "glossed over the immensity of the disruption that would occur to [DOI's] operations." Pet. App. 31a-32a. DOI has an annual budget of $11 billion and approximately 70,000 employees. See 05-5388 C.A. App. 1423. The agency manages one out of every five acres of land in the United States; provides the resources for nearly one-third of the Nation's energy; provides water to 31 million people through 900 dams and reservoirs; receives over 450 million visits each year to the parks and public lands it manages; and implements hundreds of statutorily-mandated programs. *Ibid.* To carry out

its functions, DOI has utilized approximately $1 billion worth of information technology, including approximately 100,000 computers. *Ibid.* As then-Secretary Norton explained in her declaration filed in connection with the district court's March 2004 disconnection order, "Internet communication is not merely a useful tool—it is essential to much of what we do." *Id.* at 1432.[3]

b. In recognition of the importance of information technology to federal agencies, the statutory scheme created by Congress to oversee computer security in the federal government does not contemplate blanket disconnection orders. The Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. 3541 *et*

---

[3] Petitioners' assertion that DOI "never introduced any evidence of harm that disconnection from the Internet would cause them," Pet.10; see Pet. 17-18, is clearly wrong. Government witnesses repeatedly testified during the 59-day evidentiary hearing that computer networks and internet access are essential to DOI's performance of its statutory duties, and that a network disconnection order would have an extreme practical impact. See, *e.g.*, 05-5388 C.A. App. 1436 (DOI "relies upon the Internet heavily to collect the information necessary to process rents, royalties, and bonuses owed to the federal government, including those for Indians."); *id.* at 1438 ("[I]f we have to shut down from the Internet, the oil and gas companies cannot put their production data into the system, and, therefore, we can't collect the royalties and put that money into the Treasury and, therefore, royalty checks are not paid out to all the allottees."); *id.* at 1446 ("We rely on computers to do almost everything we do."); *id.* at 1443 (explaining that, because DOI provides electronic financial services to other federal agencies, a network shutdown "would have a severe impact on financial management for large portions of the federal government"). Indeed, the district court acknowledged that DOI "put on evidence of the ways in which the department's operations were disrupted by this Court's last disconnection order" and of "the effects that a loss of Internet connectivity would have on the department's ability to service its customers, many of whom are other governmental agencies." Pet. App. 275a-276a.

seq. (Supp. III 2003), establishes a "comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations." 44 U.S.C. 3541(1) (Supp. III 2003). Under FISMA, each agency is responsible for providing information-security protections "commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems." 44 U.S.C. 3544(a)(1)(A) (Supp. III 2003). The Act directs agencies to assess "the risk and magnitude of the harm that could result" from potential security problems, and to implement "policies and procedures to cost-effectively reduce risks to an acceptable level." 44 U.S.C. 3544(a)(2)(A) and (B) (Supp. III 2003). Agency risk assessments are subject to independent auditing by the agency's IG rather than to judicial review, 44 U.S.C. 3545 (Supp. III 2003), and final authority to "approv[e]" or "disapprov[e]" an agency's information security plans rests with the Office of Management and Budget (OMB), 44 U.S.C. 3543(a)(5) (Supp. III 2003); see 44 U.S.C. 3502(4); 44 U.S.C. 3542(a) (Supp. III 2003).

FISMA thus reflects Congress's recognition that, because all security is relative and federal resources are finite, the government's identification of appropriate security measures requires a series of administrative risk determinations and judgments as to how best to allocate limited funds. Because of the critical role of information technology in administering government programs, neither FISMA nor OMB guidance contemplates that computers—let alone an entire Cabinet agency's computer networks—should be disconnected when potential security threats are discovered. To the

contrary, FISMA requires that an agency's information security program must include "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency." 44 U.S.C. 3544(b)(8) (Supp. III 2003). This statutory framework enacted by Congress to address issues of information security on a government-wide basis—including for computer systems in such programs of importance to individuals as Social Security—must be respected by any court confronted by a request for an injunction disrupting an agency's computer operations, whether in the context of Indian affairs or other government programs.

c. As the court of appeals observed, petitioners produced "no evidence showing that anyone has already altered IITD by taking advantage of [DOI's] security flaws, nor that such actions are imminent." Pet. App. 30a. This Court "has repeatedly held that the basis for injunctive relief in the federal courts has always been irreparable injury and the inadequacy of legal remedies." *Weinberger* v. *Romero-Barcelo*, 456 U.S. 305, 312 (1982). Yet despite ample discovery and a 59-day evidentiary hearing, petitioners failed to demonstrate that anyone other than contractors for the IG and the former special master—professional "hackers" equipped with extensive resources and immunity from criminal prosecution, cf. 18 U.S.C. 1030 (2000 & Supp. IV 2004)—has ever succeeded in penetrating DOI's computer systems housing or providing access to IITD. Nor is there any reason to conclude that manipulation of that character is likely to occur in the near future, or that any such abuse that might occur would go undetected or cause irreparable harm. As the court of appeals observed, "Even if someone did penetrate [DOI's] systems and

alter IITD, we have been shown no reason to believe that the effects would likely be so extensive as to prevent the class members from receiving the accounting to which they are entitled." Pet. App. 30a. Absent "something more than a list of vulnerabilities," *id.* at 31a, the court of appeals correctly prevented the district court from injecting itself into the day-to-day management of DOI's computer security.

The district court also made no serious effort to reconcile its injunction with the public interest. Cf. *Romero-Barcelo*, 456 U.S. at 312 ("[C]ourts of equity should pay particular regard for the public consequences in employing the extraordinary remedy of injunction."). Although the district court found that disabling DOI's electronic communications would serve the public interest, see Pet. App. 278a-279a, the court of appeals correctly characterized that proposition as "dubious," *id.* at 33a, given "the far-reaching effects this order would have on [DOI's] operations," *id.* at 34a. And because "maintaining adequate computer systems * * * is critical to the completion of an adequate accounting," 391 F.3d 251, 257 (D.C. Cir. 2004), disabling DOI's computer networks would have delayed the very accounting activities that this lawsuit seeks to accelerate.

2. Petitioners contend (Pet. 11-19) that the court of appeals failed to give adequate deference to the district court's application of the factors bearing on the propriety of injunctive relief, and that the court of appeals' decision therefore conflicts with decisions of this Court holding that an abuse-of-discretion standard applies to appellate review of an injunction. That claim lacks merit. The court of appeals stated that it would "review the decision to issue an injunction for abuse of discre-

tion." Pet. App. 29a. And, while the court of appeals did not expressly state that the district court had "abused its discretion" in assessing the relevant factors, that determination clearly infuses the court of appeals' analysis.

Thus, the court of appeals observed that petitioners had identified "no evidence" of actual or imminent alterations of IITD and had given the court "no reason" to believe that any such abuses would lead to irreparable harm. Pet. App. 30a. It stated that "[t]he district court seemingly disregarded the harm an injunction would cause to [DOI] and those depending on [DOI's] services." *Id.* at 31a. The court of appeals observed that it could not "find any support whatsoever for the district court's belief that merely allowing [DOI] to reconnect its computers for five days per month would be sufficient to avoid serious harm." *Id.* at 33a. The court stated that the district court had "failed to explain" its reasons for concluding that the injunction would serve the public interest, and that "[t]he overbroad definition of IITD used in the [injunctive] order makes clear that the order was not tailored to protect the integrity of the specific data [DOI] will need to perform an accounting." *Id.* at 34a. The court of appeals was "confident that the harm [DOI] would immediately face upon complying with the disconnection order outweighs the class members' need for an injunction." *Ibid.* Those criticisms of the district court's analysis, coupled with the court of appeals' express recognition that an abuse-of-discretion standard applied, make clear that vacatur of the injunction did not result from the court of appeals' application of an insufficiently deferential standard of review. Indeed, in another opinion in this case issued on the same day, the court of appeals described the instant ruling as one in

which it had found an abuse of discretion. See 455 F.3d 317, 334 (D.C. Cir. 2006), petition for cert. pending, No. 06-868 (filed Dec. 19, 2006).

3. Petitioners contend (Pet. 19-21) that the court of appeals improperly required them to establish *with certainty* that class members would suffer irreparable harm absent an injunction, rather than requiring petitioners to demonstrate a substantial likelihood of such harm. That claim lacks merit. Although the court of appeals stated in passing that petitioners had not shown that they would "necessarily" suffer harm, Pet. App. 30a, the court also observed that "[a]t the very least, something more than a list of vulnerabilities is required to show that the class members may be harmed," *id.* at 31a. The court further explained that, "[w]hile the class members may face some risk of harm if IITD housed on [DOI's] computers were compromised, we have not been shown that this possibility is likely, nor that it would substantially harm the class members' ability to receive an accounting." *Id.* at 34a. Those statements make clear that any imprecision in the court of appeals' description of petitioners' burden did not affect the outcome of this case.

4. Petitioners contend (Pet. 22-29) that the fiduciary nature of DOI's relationship with trust beneficiaries rendered ordinary principles of judicial review of agency action inapplicable to this case, so that the district court was authorized to dictate the agency's priorities in building its computer networks and allocating scarce resources. In petitioners' view (*e.g.*, Pet. 26), the court of appeals' willingness to accord deference to DOI's discretionary decisions was inconsistent with the existence of a trust relationship. That claim lacks merit.

a. As the court of appeals explained, petitioners' suit is founded on the Administrative Procedure Act (APA), 5 U.S.C. [illegible] *et seq.*, which limits judicial review to "addressing specific agency action or inaction." Pet. App. 12a. Although the existence of a trust relationship may bear on the court's application of the familiar "arbitrary or capricious" standard of review, the government in administering statutes governing trust assets retains significant discretion to decide how best to accomplish its assigned tasks. See *id.* at 8a-9a (quoting *Firestone Tire & Rubber Co.* v. *Bruch*, 489 U.S. 101, 111 (1989)), 13a; see also, *e.g.*, *United States* v. *Mason*, 412 U.S. 391, 398-399 (1973). In performing its trust responsibilities, moreover, DOI was required to remain cognizant of its competing legal obligations. Cf. *Nevada* v. *United States*, 463 U.S. 110, 142 (1983). Thus, in making its own determination whether disconnection of agency computers was an appropriate means of securing IITD, DOI was obligated to consider the effect of such measures on other agency programs. See pp. 10-12, *supra*. The court in an APA case cannot appropriately conduct de novo review of agency judgments concerning the manner in which competing priorities should be balanced, nor can it direct DOI to pursue IITD security to the exclusion of all other governmental objectives.

Describing the limits on judicial review imposed by the APA, this Court recently observed:

> If courts were empowered to enter general orders compelling compliance with broad statutory mandates, they would necessarily be empowered, as well, to determine whether compliance was achieved —which would mean that it would ultimately become the task of the supervising court, rather than the agency, to work out compliance with the broad statu-

> tory mandate, injecting the judge into day-to-day agency management.

Norton v. *Southern Utah Wilderness Alliance*, 542 U.S. 55, 66-67 (2004). Consistent with that admonition, the court of appeals correctly held in this case that the APA does not authorize the district court to appoint itself the de facto administrator of computer security for DOI.

b. In any event, even private trustees "are generally free of direct judicial control over their methods of implementing" their fiduciary responsibilities. 392 F.3d 461, 473 (D.C. Cir. 2004) (citing Restatement (Second) of Trusts §§ 186-187, at 399-402 (1959)); see Pet. App. 8a-9a; *Mason*, 412 U.S. at 398-399. And because the expenses incurred in administering a private trust are generally paid by the trust itself, decisions concerning appropriate measures to secure the trust corpus necessarily require a cost-benefit analysis. 392 F.3d at 473. An injunction of the type issued by the district court therefore would be inappropriate even in the context of a private trust. Indeed, as the court of appeals explained, if petitioners were entitled to injunctive relief in these circumstances, "nearly any system administrator who maintains data for private trusts could be in danger of facing similar claims for relief, as only the unreachable goal of perfect security would be sufficient to counter general fears of data tampering by internal threats or external hackers." Pet. App. 31a. Petitioners' proposed analogy between DOI and a private trustee therefore provides no sound basis for the injunction entered by the district court.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

PAUL D. CLEMENT
Solicitor General

PETER D. KEISLER
Assistant Attorney General

ROBERT E. KOPP
MARK B. STERN
THOMAS M. BONDY
ALISA B. KLEIN
MARK R. FREEMAN
ISAAC J. LIDSKY
Attorneys

FEBRUARY 2007